Tiger Team
Draft Transcript
June 10, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Good afternoon, everybody, and welcome to the first meeting of the privacy and security tiger team. Just a reminder that this is a federal advisory committee. It's being operated in public, and there will an opportunity at the close of the call for the public to make comments, and there will be a transcript made available on the ONC Web site. And also a reminder to the tiger team members, if you could please remember to identify yourself for attribution. With that, I'll do a quick roll call. Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – eScription – CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell?

Gayle Harrell – Florida – Former State Legislator
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Josh Lemieux for Carol Diamond?

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carl Dvorak or Judy Faulkner?

Carl Dvorak – Epic Systems – EVP
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carl is here. David McCallie? David Lansky?

David Lansky – Pacific Business Group on Health – President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Neil Calman? Rachel Block? Christine Bechtel?

Christine Bechtel - National Partnership for Women & Families – VP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston? Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joy Pritts?

Joy Pritts – ONC – Chief Privacy Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
With that, I'll turn it over to Deven and Paul.

Judy Faulkner – Epic Systems – Founder
Judy Faulkner is here too.

Deven McGraw - Center for Democracy & Technology – Director
Great. Terrific. Paul, do you want to start?

Paul Egerman – eScription – CEO
Sure. I'll start by first saying good afternoon. Thank you to the members of the tiger team who are working in what is the very intense process, and thank you to the members of the public who might be listening to our call. This is an intense process. It was put together by Dr. Blumenthal to include members from the standards committee and the policy committee to really look very carefully at a number of issues related to privacy and security related to NHIN, to directed exchange, and to try to see if we can make some significant progress. It's been one of those issues where people have said for a long time that if we just got the right people in the room, we could make a lot of decisions very rapidly, and so what we're hopeful is if we do have the right people in this, at least, virtual room to do that.

What we're going to be doing today in the agenda, first to give you an overall view of our agenda, we're sort of like on a parallel path, so we're trying to do two things at once. What we're trying to do is create what we're calling a framework document that describes privacy and security policies for various

exchange architectures involving HIOs, healthcare information organizations, and so that's one thing that we're doing. In parallel with that, we're trying to be responsive to a series of actually fairly detailed and specific policy questions that are arising from an NHIN Direct group that is working to create a pilot project on a project called NHIN Direct. Those are the parallel paths.

In this case, we're going to start on the NHIN Direct, which is also sometimes called the message handling policy, so we'll be going through some of those things. The other thing that we want to do on this call also though is something that Latanya Sweeney had asked at our administrative call was to see if we could have a presentation on NHIN Exchange, which I think was previously called NHIN Connect, to make sure that we are all at a starting point. And we had asked ONC if perhaps Mariann Yeager could do that overview. Is Mariann on the call yet?

Mariann Yeager – NHIN – Policy and Governance Lead
I am on the call. Hello.

Paul Egerman – eScription – CEO
Terrific.

Deven McGraw - Center for Democracy & Technology – Director
Terrific.

Paul Egerman – eScription – CEO
Did you have any comments, Deven, or should we just go ahead?

Deven McGraw - Center for Democracy & Technology – Director
No, Paul. I think you summarized it very nicely. Thank you for letting me hand that off to you.

Paul Egerman – eScription – CEO
Terrific. Mariann, the first order, just to make sure we're all grounded before we dive a little further into NHIN Direct, could you give us a very brief overview on NHIN Exchange?

Mariann Yeager – NHIN – Policy and Governance Lead
Absolutely, and thank you all very much for inviting me to chat with you. ONC really initiated work on the Nationwide Health Information Network quite a while ago, five, six years ago, back in 2004. The activity started with a request for information and then was followed by prototype architectures where there were different approaches that were prototyped, tested, and demonstrated, and then a particular approach was sort of … and sort of tested through the past couple of years through trial implementations. That has since evolved into a production activity that we call NHIN Exchange.

We did actually provide a couple slides just to give you all something to point to, and we don't have to go through each of those in much detail, but I think you all probably are pretty familiar that the NHIN, as it's described today, is actually very much consistent with the concept of the NHIN originally, which is looking at the set of standards, policies, and services that enable the Internet to be used for secure exchange of health information. And so NHIN Exchange is really the first iteration of that in exploring how a model for HIE could be used to meet a particular set of use cases. Some of those that work early on were sort of tested, evaluated to evaluate how a broad set of AHIC use cases could be implemented, but really what we have today is, I would say, a subset of that.

If we think about, and I think this is slide three, where the exchange activity sort of fits in the spectrum, I think folks tended to think of the use case, the direct project of exploring as more on a simple exchange,

simply as secure routing of information between providers that are sort of unidirectional and what not. The exchange is more or less is supposed to represent a more robust set of functionality and capabilities, so presumably since it involves query retrieve and document submission and a myriad of different use cases and flows that the presumption is that there are sort of more robust set of building blocks for NHIN that fit in that.

If we look at the fourth slide, it is important to take a look at how ONC is organized to support the nationwide health information network, and so there are a series of policy and governance activities, including the FACA activities in developing policies and governance and rulemaking and as well as ONC is actually supporting the policy and … oversight processes for the production exchange. A lot of what this group probably has been exposed to and what the public has heard about more recently is more on the standard services and specification side and the technical side, and so there is a technical element of what's going on with Direct and Exchange and may change … and as well as software. I think, Paul, you've mentioned Connect earlier. That's really the software that's used for exchange, but there is also a whole host of policy activities to support that broad spectrum.

Really, I think this group was most interested in understanding what this exchange is, and what it's all about. The NHIN Exchange exemplifies, I would say, the initial concept or initial implementation of NHIN standard services and policies as a network of networks. What that means, practically speaking, is that there are a group of entities that came together that are securely exchanging health information using NHIN standards, an existing set of NHIN specifications, and an existing set of NHIN policies. They were developed for this particular scenario.

Some may have applicability to the scenarios you're considering, others may not, but essentially these entities are network entities. That means they represent not necessarily end users, but connections of or aggregates of those users that interact with each other. It allows these participants in this exchange to really interconnect. Instead of implementing point-to-point per se that by adopting NHIN standard services specifications and testing for conformance interoperability, that there's a way to get a networked effect for why you go through implementation once you're able to connect with the broad exchange.

It is Internet based, so there is a common implementation of standards and specifications with secure transport built in. Participants can either use the NHIN Connect software, which is the software that federal agencies developed to connect to the exchange, or they can use their own proprietary solutions or other solutions.

The requirements for participation in Exchange are very simple. Basically an entity comes forward with their system developed to conform with the NHIN specifications, standards, and services, and they're tested. There's the conformance testing and interoperability testing to make sure that data actually is able to flow, not only conforming to the semantics and syntax of the standards and specifications that have actually worked in practice, so there is that real world validation that occurs that … from end-to-end.

There are certain criteria for these entities that is not necessarily designed to connect. Individual provider practices is an example. It wouldn't preclude it from happening. It's certainly possible. There are clinics that joined the exchange and exchanging data today that the assumption was that it would be sort of connections or aggregators of those connections.

Once an entity goes through that process and successful, they're issued digital credentials, so they do receive a digital certificate, and they're added to a registry so that others in the exchange know who is available to transact with. Then they also enter into a trust agreement that puts forward the expectations

for trust, the responsibilities and accountability measures that they have to monitor the activity, and they do use a committee structure to help oversee and administer that.

In 2009, there are a pretty wide range of entities that have joined the exchange and there are about, we expect, probably about two dozen to the exchange … production in the next six to nine months. Right now it's the Social Security Administration, Med Virginia, which is an HIO, DoD, Kaiser Permanente, VA, CDC, and Regenstrief.

Paul Egerman – eScription – CEO
Excuse me, Mariann. I don't mean to interrupt, but the slides are not progressing on the….

Mariann Yeager – NHIN – Policy and Governance Lead
Oh, dear. Okay.

Paul Egerman – eScription – CEO
I just want to make sure everybody is able to keep up with what you're saying. I think you're onto another slide than what's on here.

Mariann Yeager – NHIN – Policy and Governance Lead
Why don't we move on to slide six, and I'll try to mention it, as we move through. So thinking about who is in production, there are a host of entities in production today. There are about four additional entities coming onboard next week, and then there'll be a gradual ramp up over time. Because there are a certain set of criteria for and requirement, and given ONC's obligation to establish a governance mechanism to NHIN, right now, during this ramp up time, folks that are able to join will do so either under a federal contract grant or cooperative agreement. Then once we conclude rulemaking and confirm the criteria for how the NHIN, all aspects of NHIN goes to Direct and Exchange and all NHIN would be governed, then it would possibly be opened more broadly.

There are three sets of capabilities supported in production today. I think the one that's probably the most widely known about is the look up and retrieval of summary records for care coordination, and that's the capability that's supported today between VA and DoD and … view our activities and many others coming onboard. There's also query and retrieval of records for the purpose of social security disability determination, and that's done under an authorization.

There are two other capabilities that are new, newest to the production realm. One is the delivery of biosurveillance reporting data. That's handled through a publish/subscribe mechanism where CDC … where data providers basically make it known that they have public health or biosurveillance reporting data. CDC subscribes to receive updates to it and so the data is routed to CDC, and that's in production with Regenstrief, and there are a number of other entities doing that for that. I think it's for H1N1 reporting right now. Then the capability that's going into production in the next week or so, I think will be of fair amount of interest to this group is actually the secure routing of quality assessment data from healthcare providers to CMS. That is using a document submission specification, so from a flow perspective, that is using possibly a different set of standards and specifications that probably … similar in terms of information flow to the work that this group is contemplating.

The next slide, slide seven, the current artifacts and resources that explain how the exchange is doing business today, so there are policy documents. There's copy the trust agreement that's available, and explanation of how the committees are acting and working. Like anything, the first time you put something in practice, this is a learning opportunity, and it's … working or not, and adjusting as we go.

There are also two services that are supported in production. There's a service registry, which is basically a list of the connected nodes in the exchange … no PHI, and it simply lists the participants in the exchange and the services they support. And then there's a certificate authority that's in production, and the specifications that have been vetted for public, for production use … as well as those under … piloted.

Just to clarify because there is so much confusion that Connect is not necessarily the equivalent of NHIN or NHIN Exchange, but it is a federally developed software solution. It's a gateway that allows federal agencies to exchange information, and so Connect actually is that solution, that technology that was just tested and validated for conformance to the NHIN specifications. And so it's one of a number of gateways that are available. It is used by the agencies listed on slide eight where it's been used for the demonstrations, as well as in production, and they're certainly ramping up significantly. And it's also available in the open source community, so private sector organizations are also interested in using them as well.

We did include just one slide to at least outline how and, on slide nine and slide ten, to just articulate how the exchange is currently supporting, and it has implemented trust, and this is something that will continue to go on over time. But there are, and this framework here was based on a recommendation from the NHIN workgroup that there be an HIE trust framework, and so what we did is kind of mapped how the exchange is implemented, the different elements in the trust framework, so you'll see that there are certain agreed upon business and legal requirements and expectations. And this highlights how and some of the key elements around that, as well as….

Paul Egerman – eScription – CEO
Can we get the slide presentation updated, so people can make sure they see this slide nine? I just want to make sure.

M
If you can just say "next slide" when you're ready to move the deck slide.

Paul Egerman – eScription – CEO
Right now I think it's on eight. There we go. Thank you. Sorry to interrupt you, Mariann. But I just want to make sure … important.

Mariann Yeager – NHIN – Policy and Governance Lead
No, that's fine. The coordinating committees and technical committees are the committee structures that the exchange set up to really oversee their activities since there is sort of a gating mechanism to make sure that folks meet a certain set of criteria and have successfully demonstrated conformance and interoperability that they serve a function there, as well as serving a coordinating function for breach reporting and addressing disputes. There are some accountability mechanisms in place that if a participant is found to not comply with the terms and obligations as a group that their participation could be suspended or terminated, and there are also other lead accountability and enforcement issues that are addressed through allocation of risk and liability. The group has also several mechanisms in place for identity assurance and authentication, as well as technical requirements.

If you go to the next slide, on slide ten, it just gives just a visual of how the exchange and where the exchange has implemented trust, again, within the context of the HIE trust framework. That is just a high level overview of how the exchange is sort of looking today. It's evolutionary for sure and will continue to adapt, particularly as the FACA puts forward additional recommendations and definitely as ONC is useful with governance and rulemaking.

Paul Egerman – eScription – CEO
That's terrific, Mariann. Thank you so much. Excellent job. Do people have questions for Mariann?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have a question. I just want to be explicit in my use of these terms. Is the key difference between the term NHIN and NHIN Exchange that the NHIN Exchange is a group of organizations who have signed a DURSA? What's the difference between those two terms?

Mariann Yeager – NHIN – Policy and Governance Lead
The NHIN would be the list of standards and specifications and services and policies that ONC puts under the umbrella of NHIN, meaning those things, those core elements that are needed for Nationwide Health Information Exchange. The NHIN Exchange itself is the group of entities that have been put together to implement a set of those standard services and policies that the way they've elected to implement the policies and accountability and oversight and whatnot, some of that has been codified ini the DURSA, the Data Use Reciprocal Support Agreement, which is their trust agreement, as well as other mechanisms that are highlighted here. So I would say that's a pretty good characterization that is a group of entities that came together, and they're the participants that have founded DURSA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you.

Judy Faulkner – Epic Systems – Founder
This is Judy, and I have a question too. If I'm a patient going to a healthcare provider, what does this mean to me as a patient and my data? And not with respect to how it's kept or the technology of health kept for the privacy with health. But I'm a patient in Madison, Wisconsin. I go to Chicago, Illinois. What does it mean to me?

Mariann Yeager – NHIN – Policy and Governance Lead
It means that a patient would have the ability to have their information accessible at the point of care for providers, irrespective of geography, and one thing I didn't really get into, there are a lot of topics here I know you all would probably be keenly interested in, and we're barely able to touch on it. But there is a concept of an autonomy principle that the rules and policies and laws that apply to the party requesting the data, the provider that might make a query for data, that they're subject to whatever set of rules and policies that exist at that point of care.

Paul Egerman – eScription – CEO
I'm sorry. Could you clarify which point of care, the requestor or the requestee? Which are the rules that apply?

Mariann Yeager – NHIN – Policy and Governance Lead
It would be the rules of the healthcare provider requesting data.

Joy Pritts – ONC – Chief Privacy Officer
Mariann, I'm going to have to jump in. The way I read it was that it's the rule of the – the way I read the DURSA is it's the rule of the holder of the data.

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's the way I read it too, Joy.

Mariann Yeager – NHIN – Policy and Governance Lead

That's correct. I probably just misinterpreted the question, but that is correct.

Paul Egerman – eScription – CEO
That's what I was trying to understand. Thank you.

Mariann Yeager – NHIN – Policy and Governance Lead
Sorry.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. My question really goes to the heart of things, as the privacy and security of this entity. It already is – and now I want to clarify – this already exists. People are exchanging data within it currently, and it's basically run under a DURSA agreement between the individual parties. What privacy and security standards have been put in place is what we are going to be doing, I would assume, is going to have a significant impact on what happens here. I have a great concern knowing that this exists out there already. People are exchanging data on it without governance models, without privacy and security standards built in, and things of that sort, other than simply by a DURSA or written agreements between different people. Tell me the relationship and the impact … is going to have on it.

Mariann Yeager – NHIN – Policy and Governance Lead
There are several questions in there, and I think they're very valid questions. This activity that's in production today, and it's in limited production, so it's just the folks that were listed in an earlier slide that are exchanging data with each other in a very limited capacity. It's in early ramp up stages, so just to give a sense of scope, there is one agreement that they have all signed. They have all submitted to an in term governance structure. The privacy and security requirement and the requirements that they have in place are implemented in several places. One is that it puts forward expectations in the legal agreement that each party abides by applicable law. So, at a minimum, each party has to abide by applicable law.

It further stipulates that if you're a covered entity, you have to abide by HIPAA. If you're a business associate, you have to abide by HIPAA. If you're a governmental entity, you have to abide by additional requirements. And for the federal agencies, that's FISMA and privacy…. If you're none of those, if you're not a federal agency, and if you're not a covered entity, and if you're not business associate, there is a contractual standard of performance that is HIPAA.

We worked with the Office for Civil Rights. I will say that this is just with respect to the contract. The agreement itself went through about a four-year developmental process. It went through at least four different federal clearance processes, both within HHS, including active engagement with HHS, Office of General Counsel, Office for Civil Rights, and the federal agencies that are signatories to it … went through very rigorous clearance processes within the Veterans Administration, Department of Defense, and Social Security Administration.

Privacy and security were absolutely fundamentally baked in at the top of the list, not just a legal agreement, but also in the in term governance mechanisms that there are actually additional processes above and beyond applicable law the parties have agreed to, such as a one-hour breach notification in the event there's a suspected or a known breach. They will actually report to each other that within 24 hours. That's above and beyond applicable law.

And I think that the participants may be held to a slightly higher bar than exists today. And, if anything, I think this experience has proven that they were not comfortable relying just on applicable law. That they felt they needed additional governance. They felt they needed additional policies and procedures, which are on the public Web site where the coordinating committee and the technical committee actually have

additional policies and procedures around that. And there are processes to turn them on and off, and dispute mechanisms and what not. In addition, there were security mechanisms built into the specifications themselves.

There was an important body of work, and I'll just touch on it now because I think this is going to be of interest to you all, and I'm keenly interested to see what you come up with where we did explore the additional expectations around information security that a participant should need to abide by individually, not just obligations to each other, but individually to be a good data steward, to have a good security practices. That's a much harder nut to crack. I would say there's some really good analysis on work in that area, but very challenging to get to the solution without some policy guidance at the national level.

Gayle Harrell – Florida – Former State Legislator
Paul, this is Gayle again. I think that after hearing all this, we need to have those documents and see those things. Why are we reinventing the wheel?

Deven McGraw - Center for Democracy & Technology – Director
They're on the Web, Gayle. Again, it's entity-to-entity agreement, and so it was particularly designed for NHIN Exchange, and we certainly want to deal with those issues when we deal with that particular model of Exchange, but we can also make them available to folks so they can see and compare what this team has come up with over many years versus what we're contemplating for directed exchange.

Paul Egerman – eScription – CEO
Yes, so if you could….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Deven, this is Wes.

Deven McGraw - Center for Democracy & Technology – Director
Hello, Wes.

Paul Egerman – eScription – CEO
Hold on a second. Wes, just hold on a second. To make sure we follow up on Gayle's comment, can we get the Web address sent out to us or something to make sure people can get access to this?

Gayle Harrell – Florida – Former State Legislator
Yes.

Mariann Yeager – NHIN – Policy and Governance Lead
Absolutely. It is on the Web, and we'll send specific directions because it is on a particular portion of the Web site. And I will say, I think, I don't know if it was Gayle or someone else who had asked how might this group's work affect that. This is learning, and if there are recommendations that are put forward through the FACA process, and ONC is looking at the NHIN at the highest level, and so it's assumed that this activity will change.

Paul Egerman – eScription – CEO
Sure, but I think Gayle has got a good point too. You've also learned some things, and we should build on that foundation too, so that's helpful. I'm sorry. I didn't mean to interrupt you, Wes … question.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
No, that's fine. I just know I had to be pushing to get a word in, so I could get my place in line.

Deven McGraw - Center for Democracy & Technology – Director
You're up.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
A couple of questions: One, the NHIN Connect software has—this is not a question—has proven to be a valuable resource to a lot of people, many of whom are not participating in the NHIN Exchange. That is, they have an ad hoc exchange problem they need to solve, and they find the software a useful tool for doing that. The question is, for those that are participating in the exchange, is it fair to say that they are abiding by all of the bullet points on your slide seven? And I'm particularly interested in things like the standards for conveying the policy of the holder of the data to the entity that's requesting the data and then enforcing that policy at the end that's requesting the data. Then I have another question.

Mariann Yeager – NHIN – Policy and Governance Lead
Wes, what you're speaking to is on slide seven, the list of production specifications. Those are in fact supported in production. I think the only one, and I'll have to check. I think what you're talking about specifically would be addressed under the access consent policies, which is how those consent rules would be conveyed between participants, so that capability exists. I think that's just being rolled out because folks have been exchanging data since 2009, and so that is a specification that I think has been…. But they all support the authorization framework specification, which in fact passes forward the purpose for the request or the purpose for the information being exchanged … role, and all kinds of information so that information is, today, being used to enforce policy, both on the sending and receiving side.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think I'm restating what you said, but just correct me if I'm not. For those issues of dynamically describing the authorization associated with some data, and having that follow and be enforced through the network, there are technical standards that are coming into production now, but to this point that's been done through some sort of blanket policy substitute as opposed to getting that full richness of control that the standard would allow.

Mariann Yeager – NHIN – Policy and Governance Lead
I think there's a nuance to what you're saying. On the authorization framework, there is some core information that is being conveyed in SAML assertions that allows the sender/receiver on both ends of the transaction to have information that apply their policies specific to the issue of conveying more granular requirements around consent. I believe that is the one that's being rolled out, but it has been adopted and it is in production and what not.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks.

Mariann Yeager – NHIN – Policy and Governance Lead
Does that make sense?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Up until and you describe transmitting information, quality information to CMS, I believe it would be a fair summary to say that the head of document standard protocols that comprise NHIN or being used by NHIN Exchange previously had no case that was purely a push. That there was the case of I request information and receive it back. And there was the case of I subscribe to future information about this

person and receive it when it's available or this entity … available. But there was none. I just have it. I want to send it to them, so no request – the request is out of channel. It's offline.

Mariann Yeager – NHIN – Policy and Governance Lead
Correct, and that will change when CMS goes into production. That's correct, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But that will be sort of a many to one kind of push at that point where it's one receiver and presumably hundreds of thousands of senders.

Mariann Yeager – NHIN – Policy and Governance Lead
Correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks.

Paul Egerman – eScription – CEO
This is an excellent presentation, Mariann, and fortunately I think we could probably do a lot more questions if we wanted to. But, unfortunately, we have sort of a very tight agenda.

Mariann Yeager – NHIN – Policy and Governance Lead
I know you do.

Paul Egerman – eScription – CEO
I just want to thank you very much for presenting, and I also want to thank you for being so diplomatic in correcting me when I used NHIN Exchange and NHIN Connect wrong in terms of terminology, but I understand the difference now, so a great presentation, and I'm sure we'll be back. If the members of the team have some questions that were not answered and didn't get time to answer, send them to Deven and me. We'll forward them on to everybody and make sure that we get your questions answered.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Mariann, I suspect we'll be connecting with you more when we delve into these issues in more detail when we get to – when we're able to spend more time on conversations about these more robust exchange models.

Paul Egerman – eScription – CEO
That's right.

Mariann Yeager – NHIN – Policy and Governance Lead
That sounds good, and if there's ever a time you're all interested in testimony or having different subject matter experts, we can definitely bring … to the table either online or offline. Thank you very much.

Paul Egerman – eScription – CEO
Terrific. Thank you, Mariann. The purpose of this whole discussion was just to make sure that everybody is grounded in the sense that we all have the same sort of level of understanding that this exists and that NHIN Exchange exists, and that we're talking about this other endeavor, initiative called NHIN Direct. Joy and Deven, correct me if I do this wrong, but NHIN Direct is really sort of a pilot project that we're trying to do. As Wes said, it includes certain scenarios that aren't currently included in NHIN Exchange. Did I say that right, Deven and Joy? Do you want to add anything to the description … NHIN Direct and NHIN Exchange?

Joy Pritts – ONC – Chief Privacy Officer
It sounds good to me.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I think that's exactly right, but it's being viewed as an important pilot, obviously, or we wouldn't be here having these conversations.

Paul Egerman – eScription – CEO
That's right.

Joy Pritts – ONC – Chief Privacy Officer
Deven, I think you're too close to the phone.

Deven McGraw - Center for Democracy & Technology – Director
You know what I did? I put my do not disturb button on. How about this?

Joy Pritts – ONC – Chief Privacy Officer
That's better. Thank you.

Deven McGraw - Center for Democracy & Technology – Director
Thank you. Sorry about that.

Latanya Sweeney – Laboratory for International Data Privacy – Director
This is Latanya. I do have one question. What exactly is the relationship between ONC and NHIN Direct?

Paul Egerman – eScription – CEO
Joy, can you answer that?

Joy Pritts – ONC – Chief Privacy Officer
ONC is working through Arien Malec, is working with private vendors. It's a public/private effort to look at developing these protocols.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Is this only one of such a venture, and does ONC have money on the table here?

Joy Pritts – ONC – Chief Privacy Officer
I believe that I am not the expert on NHIN Direct, but it is my understanding that the "money on the table" here is just through the support of Arien Malec and the people who are supporting that effort.

Gayle Harrell – Florida – Former State Legislator
I have another question also. Are the policies that we are going to recommend going to have an affect on NHIN, NHIN Exchange, NHIN Connect, NHIN Direct? I'm assuming that we are going to be recommending overarching policies and procedures for anyone involved in Exchange. Am I correct?

Joy Pritts – ONC – Chief Privacy Officer
Ultimately that is, I think, what the goal is here.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think that's correct, although they may have slightly different twists to them depending on the model and depending on how specific we are in those policy recommendations. Gayle, I think you're exactly right, and that's one of the reasons for doing, for sort of proceeding along two tracks, taking up specific issues raised by NHIN Direct that may or may not be applicable to other models, and then thinking of a framework for exchange more generally.

Paul Egerman – eScription – CEO
Right, although some of the enforcement issues are different.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
Because if you look at who are the participants in NHIN Exchange, you've got the Veterans Administration and this meaningful use stuff doesn't apply to them. And so there are some issues that are different. But certainly we're free to make whatever recommendations we want to make to ONC, and so hopefully we will have an impact on the entire process.

What I'd like to do here to keep the agenda moving is to make sure everybody understands, I mean, Latanya asked a good question about is this other group NHIN Direct. The NHIN Direct group, as we know, is ahead of us, and they're choosing technical solutions for NHIN Direct. They actually have an intensive week going on this week. There are a number of people, I think, up at Microsoft today and tomorrow, and choosing among four alternatives.

Now among these four alternatives, the standards committee had a workgroup, the review committee that Dixie headed, and it actually made a recommendation yesterday. Its recommendation narrowed the group from four to two, and it's actually probably narrowed a little bit more than that. Basically Dixie's recommendation seemed to like REST and seemed to like some aspects of what was called the SMTP implementation. It's not necessarily binding on what the NHIN Direct group might decide today and tomorrow, but that was at least the recommendations I heard to the standards committee yesterday. Did I get that right, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right. Yes. We selected the REST implementation of the four and suggested they add aspects of the SMTP.

Paul Egerman – eScription – CEO
So what I wanted to do to try to help the NHIN Direct people and give them some guidance. It's unfortunate they're ahead of policy. It's not the way it should be, but I wanted to go through the spreadsheet that Dixie had sent out that has this concept of implied policies. This is sort of like the dual tracks where we're going through some of this at a little bit of a detailed level before we've got the basic policy in place, but to go through this to see if there are areas that we want to comment on, as they are making their decision.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Paul, this is Latanya. Can I just make one statement, and that is that I actually do question the ethics of the situation because it's not necessarily NHIN Direct as a finished product. We're actually moving into and becoming a part of their design process, and there are about 50 vendors out there who have put about $100 million on the table of their own money, and local decisions are being made about local NHINs, and they can't come to us, when they're trying to figure out their technical design decisions, come

to us and ask us, well, do you think we should do this, or we should do that? And I prefer to do this. What do you think? I'm not trying to set up a conversation to be disruptive to the agenda, but I did want to put it out there that I do have some serious concerns about spending, one, the activity itself and, two, the tremendous amount of time devoted to NHIN Direct without opening up to other vendors.

Deven McGraw - Center for Democracy & Technology – Director
It's absolutely not our job to bless or opine on their recommendation, I don't think. I think our job is to come up with overarching policies that can guide exchange in a whole host of models, and that all exchange, regardless of model chosen would need to meet. The exercise of ONC thinking about the specific implementation that they want to pilot as part of NHIN Direct, which may or may not be used by providers to meet meaningful use is, in my mind, a separate conversation and one that I think it would be good for us not to get caught up in quite frankly, but we do need to understand what the policy implications are of some of the models that they're choosing in order to make our policy assessments that ought to apply to all of them.

Latanya Sweeney – Laboratory for International Data Privacy – Director
But this is a crowd – NHIN Direct is a crowd sourced effort, and it means that they're basically leveraging existing technology maybe borrowed from other fields, pieced together in interesting ways, and brought forward to the table. But when you look across billions of dollars that these companies are putting out there, they have some incredibly innovative solutions that don't have anywhere near the same kind of policy issues. And so we're spending a lot of time looking at NHIN Direct as if it's indicative of the others out there, and it doesn't seem to be indicative. It's not even indicative of HIEs. Of most popular HIE models, it's not even indicative of.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I mean, I think….

Latanya Sweeney – Laboratory for International Data Privacy – Director
I don't want to derail the general….

Deven McGraw - Center for Democracy & Technology – Director
No, but I think it's a fair point, Latanya, and I think it suggests that as we are looking and formulating the policies, even if we are starting with an assessment that came from looking at the models that the NHIN Direct technical team is looking at, that should not preclude us from thinking about what the other models are that are out there. And to the extent that we have folks on the phone who can help us with some of those more innovative models that are approaching these issues in a completely different way, that would be incredibly helpful.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, this is Dixie Baker. May I just make two points here? Number one, NHIN Direct is an ONC sponsored project. Yes, it involves people from industry, but it's ONC sponsored project. You know, Arien Malec works for ONC, Doug Fridsma. It's an ONC project, that aside.

The reason why I sent the spreadsheet that we used to assess these implementations to Paul and to Deven is really that they did not – the NHIN Direct project did not start out making any policy statements. They did, in the course of the project, and in the course of developing these four implementations, make some technical decisions that really imply some policy. I see those implementations, as well as what they call the consensus requirements that they developed, as really valuable insight to inform our policy efforts because they didn't have policy, but they knew, you know, they really made some policy decisions

because they had to. You know, it was just a matter of circumstance … and all that. But the decisions that these people made are really valuable to us.

Paul Egerman – eScription – CEO
Thank you, Dixie. Let me comment also on what you said, Latanya. First, I think you raised an extremely important point. You have an excellent issue. There's a related issue too, which is sort of like who are we as a tiger team. We don't really make recommendations to anybody except the policy committee, and the policy committee is the one that actually makes the recommendations to ONC. So it's not like we have any standing to make necessarily a recommendation to this other NHIN Direct group or to anybody. We're just a workgroup of the policy committee that reports to the policy committee.

But having said that, picking up on what Deven said that we're not here to bless anything, we're not going to be approving what they've done. To me, the benefit of this, what I call parallel path or dual path to go through some of this technical detail, at the same time we're trying to do the job right and look at the high level principles, the benefit of doing it is it also gives us a chance to sort of see what the reality of it is. In other words, how these principles really do get translated into a real technical implementation, and I think that can influence a lot of what we do.

Lots of times people say, you know, the technology can't be done without the policy, but some of the times, without the policy being done first. But some of the technology people say, well, those policy people are saying policy is about understanding what the current capabilities of the technology is. That's also a problem, so I do think there's some opportunity here. But this is certainly not an ideal process to be doing this, so I think you have some very fair points.

But unless somebody wants to objective, I was intending to continue on and to go through some of these issues. Is that appropriate if I do that in this call?

Deven McGraw - Center for Democracy & Technology – Director
Correct, Paul.

Paul Egerman – eScription – CEO
Pardon me?

Deven McGraw - Center for Democracy & Technology – Director
I said go for it. Oh, wait. Is someone objecting?

Paul Egerman – eScription – CEO
Okay.

Deven McGraw - Center for Democracy & Technology – Director
Go for it.

Paul Egerman – eScription – CEO
Here's what I want to do is I don't know if we've got this on the PowerPoint that the public can see, but I've got open on my desktop the Excel spreadsheet.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Was that sent out to the committee? And if so, when?

Paul Egerman – eScription – CEO

Yes, it was probably sent out; I think I sent it out yesterday afternoon.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Wes, I'll forward it to you.

Judy Sparrow – Office of the National Coordinator – Executive Director
I'll do that, Deven. I'll take it.

Deven McGraw - Center for Democracy & Technology – Director
Thanks, Judy.

Paul Egerman – eScription – CEO
And so what I've done is I've opened it to the very first tab that's called NHIN Direct requirements. And I'm really looking at the column that's called implied policy. Are people sort of with me where I am right now?

M
Not yet.

M
Excuse me, Paul. This is…. Would you like me to bring that up on the screen?

Paul Egerman – eScription – CEO
If you can, that would be ideal.

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's awesome.

M
Judy, what time was that sent out?

Judy Sparrow – Office of the National Coordinator – Executive Director
I'd have to look, but I think it was sent out either last night or early this morning.

Deven McGraw - Center for Democracy & Technology – Director
Yes. It came from Paul Egerman.

M
Okay. Got it. Yes.

W
And it was sent out at 5:03 p.m. yesterday.

Paul Egerman – eScription – CEO
Yes, it was right at the end of the day. I remember it because I had to run to – I was running to another event, and I did my best to get it out. I hope I didn't spell anything wrong, but I may have messed up and not quite done the….

Deven McGraw - Center for Democracy & Technology – Director
Without your magnifying glasses.

Paul Egerman – eScription – CEO
Yes. That's right. In addition to doing this not quite right in terms of a process, this is also a visual fields test here to see how everybody's eyesight is. If you could do your best to look at the column that says implied policy, and the way I'd like to suggest we approach this is to look at these issues and say which of these issues are issues that we think we would like to discuss? In other words, we don't have to discuss all of them, and if we just don't discuss something, it doesn't mean we're okay with it. It just means we decide it wasn't of interest to us.

And so the issues here, the first one is X5.09 certificates. There's an issue about anchor configuration, certificate granularity, which actually I think is an issue that we should talk about the difference between an individual and an organizational entity. There's an issue about revocation, sender identification, encryption, and integrity. These issues, which are the ones that people want to discuss?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, this is Dixie. May I just explain what these four are, these four columns? The first two are from the NHIN Direct project, direct quotes from a document that they've developed, that they called consensus requirements. And the third and fourth columns are my thought. The third column, implied policies, is just my view, so it's a three-day activity. And the fourth is just my comments, so they really don't, you know, there's nothing carved in stone at all about this.

Paul Egerman – eScription – CEO
Rather than look at what it says in the implied policy, we should be really looking at the topics on the left side. Is that what you're saying?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. That third column is just my cut at it. Yes.

Paul Egerman – eScription – CEO
My question is then of these columns, of these rows, use of X.09 certificates, certificate anchor configuration, certificate to granularity, revocation, identification, encryption, ease of use, integrity. Which of those are topics that this group thinks that we should address?

Deven McGraw - Center for Democracy & Technology – Director
Well it's interesting, Paul. On one level, I would ideally want to have policy that addresses all of them, all of these. You know, in terms of – but the question then becomes, at what level. For example, if you had a policy that said exchangers must have a mechanism for being assured that the entity to which they're sending data is the right one and vice versa, recipients of data must, you know, need to be able to trust that it's coming from a source that they know. That's one level of policy. Then you dive it down to a more specific level of something that might say, though shall use X in order to do this.

I actually think the way that Dixie has got it framed here, which is that digital certificates, for example, may be used to do this. Then, if in fact those are used, are there specific requirements that we want to make sure they meet in terms of providing a sort of consistent level of trust across all users. Does that make sense in terms of this is the sort of, at what level does policy go? Does it say thou shall do X, or does it say thou shall have policies and practices in place that assure the following. Here are some recommended practices that can get you there. And if you use them, they need to meet this level of trust.

Paul Egerman – eScription – CEO

What you're saying is, in some sense, we want to address all of these. When I asked the question, what do we want to address, the issue is maybe some of these are just at too detailed a level for us to address at this level. Is that what you're…?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Let me give you – this is Dixie.

Paul Egerman – eScription – CEO
Is that what you're saying, Deven?

Deven McGraw - Center for Democracy & Technology – Director
I think it might be. I'd be interested to hear, since Dixie put the implied policies on here, what her thoughts are.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I couldn't agree with Deven more. Let me give you a specific example that really came out in this exercise. One of the implementations, for example, well, let me back up. For example, I think X5.09 certificates, anchor, granularity, all those have to do with an authentication policy, and the policy, as Deven pointed out, really should address, start at that level. What do you need to authenticate?

The example I was going to give is that one of the implementations assumed that the end user would need to authenticate itself to what they call the health information service provider, HISP, that they would need to authenticate themselves to the HISP. But the HISP, the service provider would not need to authenticate itself back to the end user. Well, that's an assumption, and I think that that's a policy we should address. Who needs to authenticate? What entities need to authenticate each other? When do you need mutual authentication versus one end? That's the granularity I think we should be talking about.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
This is Wes. Can I add something?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I am having a great ah-ha moment here, and that's that in talking about policy, we're having the same conversation when somebody from Dallas and somebody from Manchester, England talks about football, which is to say, we're using the same word for a different concept. It's always been, I think, an issue in discussions I've been involved in with Dixie for the last couple years anyways. There are very concrete things that a technician or a technical person can decide to do once somebody makes a judgment about which is the best one to do. I think Dixie calls those judgments policies.

And there is the level of policy that is a set of principles on which somebody makes that judgment, and I think that's what most of us on the committee call policies. And we are getting confused, not because those aren't both important, well-identified things, but we're using the same words to describe both of them. So if you look at the policy framework, material that we've done, you can't look at those documents and decide the policy issues that Dixie describes as policy issues, but they would be great guidance in deciding those issues.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's where I think we're having a little bit of a disconnect.

Paul Egerman – eScription – CEO
Yes, so that's excellent. Those are excellent comments, Wes, because I think you're saying something very similar to what I'm hearing Deven saying.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
This is Micky. I'm wondering, is it too simplistic to say that we want to focus on the what and not on the how?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. No, no.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
That it's too simplistic or…?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, it's not too simplistic.

Deven McGraw - Center for Democracy & Technology – Director
I don't think it's too…. I think Dixie and I were about to say that's exactly the simple way to describe what I think was the point that Wes and I were trying to make, although I admit, Dixie, that I got a little confused by you agreeing with me and then it seemed to be at the level of detail that I would put in the guidance category versus a policy category.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What I was trying to point out….

Deven McGraw - Center for Democracy & Technology – Director
Wait. Let me let Dixie respond to that, and then I think that was either Wes or Micky in the background.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I was attempting, you know, I did. I totally agreed with your first comment, and what I was trying to give you was an example of what you talked about as going down to the next level.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The top level is, you know, we need to make sure that we're talking to the right people, right? And the next level down is who needs to make sure that they – you know, who needs to authenticate themselves? But I agree with you that it's a level of granularity thing that we should start at the top level.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Neil Calman - Institute for Family Health - President & Cofounder

Deven, this is Neil.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'd like to say that I think it is too simplistic, okay, because what is one person's what is another person's how.

Paul Egerman – eScription – CEO
Who is speaking right now?

Deven McGraw - Center for Democracy & Technology – Director
That's Wes, I think.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
This is Wes, yes, and I think it's almost like goals and objectives in some frames of reference. My objective contributes to your goal, but I think we need to just decide, are we focusing on the policies that can directly guide security implementation, or are we focusing on the policies that guide the formation of the policies that directly guides security implementations?

Neil Calman - Institute for Family Health - President & Cofounder
This is Neil. This helps me try to understand the relationship between the document that Deven sent out, which was the other grid.

Deven McGraw - Center for Democracy & Technology – Director
Yes, that's our framework grid.

Neil Calman - Institute for Family Health - President & Cofounder
Right, and this grid, and I feel like I've been hanging in these two days' worth of calls because I feel like I might have something to contribute to the framework grid, but absolutely nothing to contribute at this level of technical specification, so we also might want to consider whether the right people are on the call for both of these. I mean, I don't know how many people on the call are prepared to discuss this second grid that was sent out yesterday afternoon. I know that I have nothing to contribute there. And all of that seems to me to fit into one box on the framework grid, which are the technical requirements around the safeguards.

Deven McGraw - Center for Democracy & Technology – Director
It does.

Neil Calman - Institute for Family Health - President & Cofounder
And so what about the test of the framework grid? And it's somehow somebody has got to connect these agendas. It's like if the framework grid is the big picture, then how are we going to address all of those pieces of the big picture? And I don't think this group is going to be able to do it at the level of granularity of this second spreadsheet that was sent out.

Joy Pritts – ONC – Chief Privacy Officer
You know, this is Joy. I think that what Arien was – this particular exercise is really being done at the request of NHIN Direct because they, Arien in particular, have spoken with members of the privacy and security workgroup and is trying to get some policy guidance for what they are doing, and I will apologize on behalf of ONC that this is not occurring the way that it should occur. We all kind of recognize that at this point. But I do think that there is general guidance, recommendations that this group could focus on that would be helpful for Arien.

He, I believe, is looking at some fairly general, but even general recommendations would be helpful for him. In particular, I believe he was interested in, in this group, looking at what they thought the rules should be for a HISP or the intermediary and how they could – whether, how – whether it was ever appropriate for them to be able to see patient identifiable information. If so, when? What kind of rules might be in place? If not, how you would accomplish that in general. I think that's kind of the level he was looking at.

Latanya Sweeney – Laboratory for International Data Privacy – Director
This is Latanya. I apologize for the background noise. I literally am standing in the middle of a highway with cars going all around me. If there was a picture of this, you would all crack up laughing. But I did want to say—

M
Take one for the team, Latanya.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Before I get hit by a car, I just wanted to day that the questions that Arien is asking are generalized from his perspective, but it's actually looked at in the general, are far broader than any other kinds of things, the way he's framing them. It is a kind of issue where it's still kind of over-fitted to them. One of the recommendations I was going to make to Arien is I think that they should crowd source the policy questions.

That is, engage in open forums, just like they did with the technology design to say what do you guys think we should do. And they'll get high stakes people involved, just like they did with the technology people, and they can inform us. They could come back to us and say, you know, we made these decisions, and these people supported this decision. What do you think about that? Now I'm getting off. I'll be able to hear you, but you won't hear me.

Joy Pritts – ONC – Chief Privacy Officer
That's an alternative, but that I don't believe is being pursued at this point.

Paul Egerman – eScription – CEO
Here's what I'd like to suggest we do, listening to what you suggested, Joy, which is, I'd like to, in the agenda, I did … summarize two high level issues that Arien raised. As far as this spreadsheet picking up on what everybody says, I get the sense that nobody really wants to drive through any of the detail on the spreadsheet. There were two issues I wanted to bring to people's attention from this spreadsheet that I think might be appropriate for us to comment on.

One was this issue of granularity. It's really a definitional issue where they talk about individual physicians versus individual providers, and I think the issue there is healthcare doesn't work the way people think it works where necessarily an organizational entity represents a single medical record. And they really should be, in my mind, looking at, I don't know if you want to call it virtual organizations, but they should be thinking about how people organize their medical records, and that determines how you organize certificates as opposed to the actual organizational entity because the entities themselves are complicated things.

The other observation I have about the spreadsheet is, all of their examples, especially the REST examples, require an intermediary. And I think we should be able to comment on whether or not an

intermediary should be required. If we look at directed exchange, I'm not sure an intermediary should be required.

Joy Pritts – ONC – Chief Privacy Officer
Paul, I hear what you're saying. I don't know. The last one sounds to me like a technical issue rather than a privacy and security issue. Perhaps it can be rephrased to be more of a privacy and security issue such as, you know, I'm trying to think of it. But maybe you could think of one … how to….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If I could maybe comment on that, I think that the intent was not to say that there must be an intermediary, but that there must be a player of a reasonable amount of technical sophistication in order to implement whatever the policies are, and that player may be an intermediary, or it may be the entity itself if it has that level of technical sophistication.

Paul Egerman – eScription – CEO
Was that Wes again speaking?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. That was Wes.

Paul Egerman – eScription – CEO
That to me is helpful. To answer your question as to why it's a privacy and security issue is, yes, I can see situations where it even goes back to my comment about how you define an entity, but you look at an organization like, say, Partners, that has various relationships with various medical groups and, for a lot of reasons, you can say, well, they're going to want to organization all their exchange of information so somehow it never leaves Partners because that's actually a more secure environment for them, even though there are some people there who are like sort of members of the family, but are not really. You know, they're more like in-laws, you know, in terms of family members. They're not really part of the organization.

M
Speak for yourself.

Deven McGraw - Center for Democracy & Technology – Director
You better be careful with that one. This is a public call.

Paul Egerman – eScription – CEO
I don't know if I said that right, but I think people know how that all works.

Gayle Harrell – Florida – Former State Legislator
And in some states, they can't even legally be part. They may be the physicians working with the hospitals, but they can't be employed physicians by the hospital groups, so they're legally separated even though, in another state, they may be one entity.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
Right.

Deven McGraw - Center for Democracy & Technology – Director
It does get a little complicated. I actually have an idea for how we might be able to have this discussion, thinking about it at the policy level, but also allowing these sort of more, this detailed information to help us think about what we might want to have as appropriate policies at that sort of traditional policy level versus down necessarily in the level of implementation detail. That would be the take. That column in the chart, Neil, that you pointed out that has to do with the safeguards where basically these discussions about NHIN Direct message handling sort of probably neatly fit, and think about flushing that out. For example, if you've got, you know, policy expectations for providers to be able to authenticate, how does that reasonably occur, and what ought to be the overarching requirements that any authentication system would have to meet.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
As opposed to, thou shall do X kind of response to it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Exactly.

Deven McGraw - Center for Democracy & Technology – Director
And we could tee that up. I mean, we can continue to try to parse through some of the details of this since we still have time on this call, but we can tee that up as the framework for the discussion on tomorrow, and maybe really able to make some substantial progress on what policies we're talking about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, this is Dixie. That's exactly what I was trying to suggest, and I didn't do a very good job of it, is that, going back to Latanya's comments, what you see in these first two columns is the crowd sourced policy that they came up with.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I was trying to say, given that this is how they think, this should suggest to us the kinds of things that we need to provide them guidance on. Does that make sense?

Joy Pritts – ONC – Chief Privacy Officer
Okay, so why don't we move to identifying at least one of the policy issues that we can undertake?

Deven McGraw - Center for Democracy & Technology – Director
Yes, so I would suggest that one of them would be one of the ones on the agenda, which is the degree of PHI exposure in transport, which comes up, you know, gets put into stark relief by Dixie's analysis of some of the models and what we think the appropriate policy ought to be. I'll share with you all that I

don't know if this has been true of the rest of you, but I've been lobbied pretty hard over the last two days by the different proponents of these models around this issue of PHI exposure to entities that might, in some transport mechanism, sit in the middle and route that transport. And what's a reasonable policy that ought to guide the sort of technical process for accomplishing this?

Judy Faulkner – Epic Systems – Founder
Deven, it would be interesting, I think, for us to hear the different positions at a high level, if you could.

Deven McGraw - Center for Democracy & Technology – Director
Yes. At a high level, one could foresee, and I would love some pushback on this because I'm kind of doing this off the top of my head. But at one level, you could say the policy is that if what's happening is transport, there ought to be no PHI exposed over the network, not transport.

Judy Faulkner – Epic Systems – Founder
When you say exposed over the network, what does that mean? Does that mean that nobody can see? The intermediary, for example, cannot see any PHI?

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's essentially what I mean by that. Once it's transported to the entity, of course, they need to route it. They need to do certain things with it. Obviously some exposure of PHI, for example, in the message might make sense, but not when it's being transported over.

And then another way of articulating that in a little bit of a broader way would be to sort of put a limitation principle on it, which is to say, you know, there should be only limited access. You know, only that access, which is necessary to support the transport. Then, if in fact there is access, I think we do have to think about some policies that would apply in the middle to govern subsequent use of data.

Paul Egerman – eScription – CEO
Right, but then the next level that happens is what happens if the intermediary does something to transform the data and, as a result, needs to get access to the PHI, so transform….

Deven McGraw - Center for Democracy & Technology – Director
That's right. And so that's why it makes it hard if you say no exposure to PHI over the network for models that just involve transport. Now, of course, intermediaries that perform other services, that's obviously a different issue.

Paul Egerman – eScription – CEO
Sure.

Joy Pritts – ONC – Chief Privacy Officer
Do you think it's worthwhile to start there with, assuming that intermediary is just providing transport and have people comment on how they believe what policy should apply as to their exposure or viewing, the ability to view or access the information?

Deven McGraw - Center for Democracy & Technology – Director
I do.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I can give just sort of a real life example of something we're going through just to give people a sense of what we might be talking about from a very practical perspective.

Joy Pritts – ONC – Chief Privacy Officer
Thank you.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Yes. We're right now, the Mass E-Health Collaborative, is becoming a member of NEHEN, the New England Health Exchange Network, and they basically provide secure transport functions very, very similar to what we're talking about with NHIN Direct. So the question that's arisen, as we're going through the contract with them, do you essentially look into the message between the endpoints, between the sender and the receiver? They do for syntax checking, so while they do secure transport, what they say is we do look into the message to make sure that the syntax and the structure of the content are correct because, if we don't do that with millions of transactions, I'll just come … the works, and you'll have billions and millions of errors without doing that kind of checking.

So while there is no sort of persistent data held at the center, it is purely at the machine level. Checking each message for basic structure of the content. They are, as a technical matter, going beyond whatever metadata there is to go into the message to check that. I think that's a real question of, is that exposure or not.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Paul Egerman – eScription – CEO
Micky, what do they do if the syntax is incorrect? What's the process of fixing it?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
The process is to go back to the source system and let them know that there's been a rejection and then work on what caused the rejection.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Isn't this…?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
What caused the error? Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Isn't this just a question of – isn't this the same as asking whether the intermediary has to be a business associate or not?

Deven McGraw - Center for Democracy & Technology – Director
No, not necessary, Dixie, because I see – I would like us to think first about what we think the policy ought to be, and then secondarily about how it gets enforced, and BA agreements is one potential mechanism.

Paul Egerman – eScription – CEO
Right. But, you know, picking up on what Micky said, sort of one level is the syntax checking. Then he said there's the next level, which is, not only do they check the syntax, in effect, they fix it. So what they do is they check the syntax, and they reformat the message from one standards level to another. Perhaps they change from one. You know, they translate from some – one code set or code terminology to another and then retransmit the message. You look at, say, SureScripts of some lab systems will do

that. They will reformat messages so that they can be … format, and so that's just another level. That's beyond syntax checking. It's changing the message.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Absolutely.

Paul Egerman – eScription – CEO
But … level.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Yes, and just to be clear, NEHEN does not do that. They go back to the source system and have the source system fix it.

Paul Egerman – eScription – CEO
Right. But it's sort of like we've already got three steps. There's no change. There's syntax changing. Check to make sure it looks good, but then there's really a transformation that can occur where you look at it, and you purposefully alter it. You either correct it, or you change the version number or something.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
There's also, if you're able to look at syntax without exposing PHI, I mean, that to me is the critical question no matter what you do, whether you change it or whatever. If you expose PHI in doing whatever it is you're doing, then that's a level of risk there, and….

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Yes. Dixie, how would you define expose when you say that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, if you can look at the structure of a message, but all of the data within the fields within that message are encrypted, you can check the syntax without exposing PHI.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Okay.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I think what I mean by exposure, Micky, is the ability to see information that either impliedly or expressly provides health information about a patient. So if it's name and where it's coming from, for example, although that doesn't expressly say something about that patient's health, it says if it were coming, for example, from Whitman Walker Clinic, which, for a long time in the district was this sole HIV/AIDS service provider, people would know.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Yes. No, I was getting at a different issue, which is just from a technical perspective. There seems to me to be sort of a binary question of if you go into the message or not because, by one argument you could say, if you open up the message, it's exposed by definition because you opened up the message. I guess, if the context is encrypted, then fair enough. It's still protected, even if it were sort of stilled in some way. So that's why I was asking that question.

Paul Egerman – eScription – CEO
Yes. Picking up also on what you said, Deven, isn't it enough just that you have the identification of the patient? You don't necessarily even need to know where it was going. Just as soon as you know who the patient is, haven't you sort of … wire or something.

Deven McGraw - Center for Democracy & Technology – Director
Yes. That's definitely PHI.

Paul Egerman – eScription – CEO
It's PHI. It doesn't necessarily matter … anything else … you know the patient's name.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I think you're always, at a minimum, going to have patient's name and where it came from, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But if you had a message that the header said this is from Beth Israel, and I'm sending it over to Mayo, but the payload that included the real PHI was encrypted, personally I would think that that was just, that would be fine. You're just using the information to route the message.

Paul Egerman – eScription – CEO
Yes. The analogy I'd give you since Latanya said she was just in a highway would be if you stood on the road and you saw an ambulance go by. Well, that doesn't tell you anything. But if the ambulance goes by, and it says John Doe on the outside, then you know somebody named John Doe is sick, and that's information.

Deven McGraw - Center for Democracy & Technology – Director
Yes, fair point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Can I be heard now?

Deven McGraw - Center for Democracy & Technology – Director
Yes. Go for it, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm just having trouble knowing whether I'm on mute or not. Actually, I think Paul said what I was going to say while I was trying to figure out whether I was on mute.

Deven McGraw - Center for Democracy & Technology – Director
Okay. I think we've got an interesting picture to try to resolve with one policy or maybe one set of policies that might apply to a range of exchange models, and I'm hearing a desire to place some limitations on the exposure of PHI and, at least in transport, unless I'm missing somebody. But do we need to go stronger than that? Do we want to go stronger than that in terms of what we would provide on that issue?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Can I suggest this is an interaction between policies about how information is handled and policies on how intermediaries become trusted? If we know that some weigh station along the handling of this deck

can't see who it's about, can't see anything else, then we have one level of concern about somehow authorizing that entity to be a weigh station if we think that the fundamental information is exposed, even if it's just name and what clinic it's coming from. That creates a different level of requirements in terms of certified … or somehow … can be a weigh station.

Deven McGraw - Center for Democracy & Technology – Director
That's interesting. Wes, I'm sure you'll jump in if I mischaracterize what you're saying here. But, in essence, there would be one set of policies that would apply if no data is exposed, no PHI is exposed. Not no data is exposed. Dixie, it's not sinking in yet, but I'm working on it. Then another set of policies that if in fact you're using a model that does in fact expose some PHI in order to insure that the PHI that is exposed is the minimum necessary to perform a particular function that we think is worth performing, and that there isn't any subsequent, and there are strong data retention policies that deal with how long that can persist and what else can be done with it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Exactly. I think we, given that there is this notion that we have one class of organization that is competent to handle protected health information because they do it all with their IT systems all the time, and then there are others that might come into the market to be surrogates for organizations that don't have that IT competence. Then the question that arises is how hard is it for a surrogate to come into the market? How much are we creating constraint on industry to be providing a solution through our privacy policies and choices of technology? Clearly there are arguments on both sides. That's why it's worthy of such … committee, but the notion that we would like to find a path that carefully protects patient information and minimizes the constraints on providing a solution to the healthcare industry is a very attractive one.

Paul Egerman – eScription – CEO
I'm not sure I'm getting this right, Wes, but if I'm hearing this discussion correctly, what I'm sort of hearing is this decision is not – this issue is not like a zero or a one. In other words, it's not an issue of either there is or there isn't PHI. In some sense, if there's no PHI, it's very simple. But if there is PHI that's exposed, then it's a little bit complicated. You've got to figure out, well, to what level is it exposed. What is it used for? Who is doing it? In order to determine what the policy issue.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. Another way to say it is, the question is, is it a zero or a one? Is it a zero/one decision? We know that if – we think, we suspect that if there is no clear … PHI, that there are very few rules on who can handle the data.

Paul Egerman – eScription – CEO
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
As soon as we allow for the possibility that there might be, for the reasons that were discussed earlier, then we begin to get into what is necessary public support of this in order to make it viable. Does the federal government now have to have a certification program for protected health information handlers, or is there another approach short of that that would protect the people who become exposed to this, just as a byproduct of what's being done to consumers and still minimize the entry cost into the market. It can get complicated. It may get complicated. But it's up to us to at least give the guidance on whether it needs to be complicated.

David Lansky – Pacific Business Group on Health – President & CEO

This is David Lansky. I want to throw in a similar comment on this yes or no, on or off question. It seemed to me that it's both a strategic and a jurisdictional problem. One is the strategic one. I thought, Wes, that the origins of NHIN Direct in your early blogs and the subsequent discussion were predicated on the idea that there was a class of a simple transactions with a lot of known parameters by parties who already had a trust relationship. And the original discussion didn't introduce, in my memory, third party routing addressing service that added some services to the whole transaction, as we've just been discussing.

That class of exchanges was meant; NHIN Direct was meant to flush out and provide standards and support to, which is all good. Then, recently, that process led to the reintroduction of the HISP or some other mechanism that was kind of a pass through for addressing service, and those are two classes. The addressing service versus the sort of handling service is something we should think about.

And it seems like, once we cross back into that territory, we inevitably reopen all these discussions that are very complex and have all the components of the framework and the DURSA that need to get addressed because of the potential for either mischief or inadvertent manipulation of the data at that routing function once you've gone outside of the encrypted point-to-point messaging where we started. I'm wondering, in terms of this yes or no, on or off question. One other approach to it is to say there's a class of architecture or service structures that do not engage the full range of policy difficulty and, therefore, can be expedited, so to speak, or can be implemented efficiently and affordably between certain types of systems or providers.

Then there's another class, which may be the much larger one, that sooner or later you bump into all these issues, and you really need a fully flushed out and multicomponent framework for. And so I think the bottom line question is, is there an easy class that we can solve quickly and let Arien start running, or do we have to come back and figure out all this stuff about the HISPs, which then goes to my second point, which is jurisdictional. Are we taking, as an assumption, that this is a federal role to say here is the policy framework and the policies, which must be rolled out across the entire national infrastructure down to the lowest level of point-to-point exchange, or are we saying here's a federal certification or a route authority function, and then we're going to hand off to Nebraska a set of opportunities or responsibilities, and they can do whatever they want within Nebraska? How do we granulate that because I don't know whether this committee, the tiger team, needs to be the body that says here is the national stone tables for all these policies. I don't know. Maybe it does.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Can I…?

Deven McGraw - Center for Democracy & Technology – Director
Go for it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
There are actually two questions you raise. One of them is, in essence, addressing, and that is, how do I get the necessary information to send this information from the emergency department in Kansas to the pediatrician in Boston or whatever it is. And the second is trusting of the handling of the data. The first question, in my blogs, I said that in a local probably one big enough to make a dent in the requirements to meet meaningful use operationally, that can be done through a channel. But we recognize from the start, and we had hearings about directories that were related to the issue of when I begin to go to a third party to find the address, how do I understand that I can trust that third party? Generally, the third party that provides addresses may or may not be the same third party that handles the data, but you can treat it as a separate set of requirements, and if entity does both, then they meet both requirements.

The second one is handling the data. The presumption at the level when we started was that the data would be, no clear text data would be available going across the Internet. In the debate that has come up, some of the people who are debating the required functionality are arguing for the necessity for clear text metadata, and so the question has been come up. Is that a big obstacle? Is it not? Does it justify much more elaborate protocols, much more elaborate business set up or not? And Arien is looking for guidance, I think, on that issue.

Paul Egerman – eScription – CEO
What you said there, Wes, was a number of things. One is, as I look at this issue, I'm trying to understand. But once you expose PHI in any amount, you're sort of in a different world. But the real issue is what do you do with the data. What you're suggesting is another question. Who are you, also, and what other stuff might you be doing? Those are interesting questions to ask. Then also getting to the question Arien says, even though one intermediary approach my expose data, that's not necessarily a reason to say you can't do that approach. It just means that there's going to be some additional set of rules associated with that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. I think a good response to him would be to say if an intermediary has access to the content for whatever reason, then there are additional requirements on working with that intermediary. It better be that they have to find the DURSA and be prepared to be cut off on three days' notice by the transparency committee or whatever it's called or it could mean something else. But certainly it's a … requirement….

Paul Egerman – eScription – CEO
The real world is this happens a lot, right? E-prescribing goes through SureScripts, and SureScripts does this.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I think there's another piece to this, at least that applies in certain states that have fairly strict standards. I'm sorry. This is Micky Tripathi. For example, in Massachusetts, the presumption is even if the organization is trusted by whatever definition you want to use for trusted, you still, the discloser still has to get patient consent to authorize. It has to be authorized by patient to give the data to them. And so….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Micky, in Massachusetts then every time I go to the radiologist and the radiologist sends out a report, the radiologist has to get explicit consent from me for that specific transmission?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
No, but somewhere in that chain between the physician ordering it and wherever the imaging was done and sent back, that's where the permission happens that there is consent in that chain somewhere.

Deven McGraw - Center for Democracy & Technology – Director
Yes, but Micky, this is Deven. That's the test that there's an additional level of protection and, in this case, you've chosen consent to provide that level of protection associated with an exchange of data that involves some exposure. Am I inaccurate? But sort of along the lines of the strain of discussion, which is, when it's not exposed, that's one class, to borrow David Lansky's way of bucketing the issues. When it is exposed, that raises a certain level of concern and causes us to think about what additional protections we would put in place.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right. But just to push on this then, so let's just take this Massachusetts example, and then let's just take what I was talking about before with the NEHEN example, and that's why I was asking Dixie for this question about what does exposed mean. If it is transported through an intermediary that is allowed to do syntax checking such that I cannot tell whether the data was exposed, I mean, they viewed the data for whatever purposes, or they were just opening up the message for syntax checking that, in principle, I would need to get the consent of the patient to send up through that intermediary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
…check?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
…consent?

Paul Egerman – eScription – CEO
When you say that, Micky – I couldn't understand that, Micky. Are you saying that's the way the Massachusetts law works, or are you saying that's the way it ought to be?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I'm saying that's the way the Massachusetts law works.

Paul Egerman – eScription – CEO
But you're not saying that's the way you really like it to be. You're just saying that's just the way you have to do it….

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I'm just saying that's the way we have to do it in Massachusetts right now.

Paul Egerman – eScription – CEO
Okay.

Deven McGraw - Center for Democracy & Technology – Director
In other words, Micky, you're asking us to – you're suggesting that it's a worthwhile exercise for us to further define what we mean by expose?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
I think so, and I was just reacting to, Wes was, I think, appropriately looking at one dimension of it, which is this question of, is the intermediary trusted in some way. What I was saying was that at least in certain states like Massachusetts, even if the intermediary is trusted, there's still this threshold question of whether the discloser has the consent of the patient to send it through that intermediary to begin with.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, that alone is … send back to Arien.

Deven McGraw - Center for Democracy & Technology – Director
What?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That alone is great information to send back to Arien that if the information is accessible from an intermediary that some explicit, some states will require explicit consent of the patient to use that intermediary.

Paul Egerman – eScription – CEO
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That by itself should be very good guidance for the NHIN Direct group.

Joy Pritts – ONC – Chief Privacy Officer
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
I'm just looking at our schedule. It's about 3:40. In five minutes, we'll do the public comment. And so on this issue, what do we want to do with it? Do we want to simply say, well, it's easier if there's no exposure? If there is some level of exposure, then there's a range of solutions. In some states, that includes consent. Is that an adequate response, or do we want to dive deeper into this, and try to say, you know, define different categories, different buckets, and specifically what we should be doing, what should happen under what circumstances.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
This is Micky. I think we have to define exposure if we're going to say that.

Deven McGraw - Center for Democracy & Technology – Director
Another thing, I actually think it's worthwhile, Paul, for you and I to try to tee up some of those straw dogs, borrowing Micky's term, that we talked about. But in that safeguard category, the comment that I made earlier in the call to try to sort of look at the work that Dixie and her standards team have done, what we already have in our framework on safeguards, and try to flush that out a little bit in policy language, incorporating the good discussion that we've just had about how to transport that "exposed data". I think you're right, Micky. We'll have to drill down on what we mean by that.

Gayle Harrell – Florida – Former State Legislator
Deven, this is Gayle.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Deven, this is Josh.

Gayle Harrell – Florida – Former State Legislator
I'll like to … before we leave the absolute direct, one-to-one exchange, I want to make sure that we're not just eliminating any discussion of things like very basic things, authentication of sender to recipient.

Deven McGraw - Center for Democracy & Technology – Director
No, we're definitely not, Gayle. We just dove into the details on this one piece.

Gayle Harrell – Florida – Former State Legislator
Okay. I just want to make sure that we're not going to ignore that, that we make sure that those are all within the framework that we're going to establish.

Deven McGraw - Center for Democracy & Technology – Director
Yes, and I heard Josh for Carol on the line.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
Yes, Deven. This has been implicit in some of the comments, but I just think that the tiger team should look at it and see if there's an explicit statement that we'd want to make. And that is that the presumption that information that exposes health information being accessible on the network or by intermediaries, that there should be sort of a high threshold that the presumption should be no. You don't get it unless there's significant justification. And if there is significant justification, the parties need it then, that there are these other protections and safeguards that need to be in place before that happens.

It seems like, for example, in the common framework on the issue of querying records and matching identity, linking people to records, that the indexes to do that did not have information that exposed clinical data or personal health information, and that was a pretty iron clad rule, the limitation that I think still makes a lot of sense. And so that would be a sort of policy guidance level that says that don't expose PHI over the network or by intermediaries in certain areas. And particularly in the discovery of records and patient identity matching linking to records.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie.

Josh Lemieux – Markle Foundation – Director Personal Health Technology
The comment is that the standards should be pretty high before PHI is considered for exposure over the network or by intermediaries, and there are certain areas where it's not worth the risk.

Deven McGraw - Center for Democracy & Technology – Director
Thanks, Josh. Go ahead, Dixie. That's a good point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, excellent point. There's one more point that's been made sort of tangentially several times by Paul and others that I think we should make sure we capture, and that's the question not only of exposure. Exposure is kind of the first step, but also the integrity of the data.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That second level of, you know, if the intermediary not only sees it, but then changes it, or somehow, you know, because that introduces the second level of risk. Not only is there the confidentiality risk, but once they start manipulating it, there's the data integrity risk and associated safety concerns. I think that our policy should address both of those risks.

David Lansky – Pacific Business Group on Health – President & CEO
This is David. I agree. And I think there's kind of a Pandora's box we're going to soon open in this arena by … another HIE, which has 40% of the lab messages they have to open to fix the NPI in order for it to

get to the right place. We're going to see a lot of that, and as soon as that happens, how do we know they fixed it right, etc? I do think we cross this threshold of the exposure to the intermediary for whatever reason and there are 100 important issues that are going to fall out of that that will be tough to resolve quickly.

Paul Egerman – eScription – CEO
Right.

Gayle Harrell – Florida – Former State Legislator
One of those … is liability. We just had a huge case in Florida where there was incorrect data entered into a record and … I don't know, through an intermediary or whatever, and it wound up in a huge malpractice case, and also someone – the Board of Medicine taking action.

Deven McGraw - Center for Democracy & Technology – Director
Oh, boy.

Paul Egerman – eScription – CEO
Exciting.

Deven McGraw - Center for Democracy & Technology – Director
Cautionary tale.

Paul Egerman – eScription – CEO
This is an excellent discussion and excellent comments. I appreciate those comments, Gayle, about a real world situation. Again, I'm looking at the clock a little bit and trying to think about the agenda. Where should we be taking this discussion? Should we continue it tomorrow? In other words, is this a discussion that we have enough information right now, if we continue it tomorrow, we're going to be able to solve this and resolve something? What's the next step that we should be doing on this issue?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I have a suggestion that we're sort of – you raised it a minute ago, which is in terms of how we should proceed, which is, who is driving the questions here? Is it valuable use of the committee's time to answer a specific set of fairly well articulated questions from Arien or is it that we need to get in and go through it all and determine what all of the impacts of policy are? Or is there an A/B kind of an approach there? If we can identify specific, concrete questions, then it would certainly be a trial of our capability as a group to try to get them specific answers over the course of a couple hour call.

Deven McGraw - Center for Democracy & Technology – Director
I personally think it's A/B, and it gets to Gayle's question about whether we're going to try to resolve some of these other issues. Admittedly, we have a very tight timeframe, but that's why I suggested maybe excerpting out the matrix framework document and trying to populate it with some more of the specifics on issues that were revealed in the examination of what's going on with NHIN Direct so we can get to some of the specifics where we think it makes sense to do so, but we're progressing it also along a sort of more holistic set of policies that we think ought to be in place that aren't necessarily relevant to specific questions that Arien has asked, but are important as sort of guidepost or stakes in the ground to send a really clear message about what we want to see. Does that make sense?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Would it be fair to call that a bottom up approach to being holistic?

Deven McGraw - Center for Democracy & Technology – Director
Sure.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
In other words, what I mean by that it's easier to get a handle on a wholistic framework if you tackle some specific issues first and sort of get the storming informing part of the exercise out of the way, and then use the understanding that's developed in the specific issues to go back and approach more holistically. I'm suggesting that if that's what you had in mind, it makes a lot of sense.

Paul Egerman – eScription – CEO
That suggestion, am I hearing this right then that we would continue this discussion tomorrow on this…?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
…specific answerable questions that are smaller than what is life and at least pick one and get the answer to it at the end of two hours.

Paul Egerman – eScription – CEO
Is this the one we're going to pick?

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
Then tomorrow what we'll do is we're going to continue with this discussion and try to basically answer the question. Is that…?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Will you reformulate the question and send it out?

Deven McGraw - Center for Democracy & Technology – Director
Yes, I mean, I'd like to. I think it would be helpful if we did that.

Joy Pritts – ONC – Chief Privacy Officer
I think, in the meantime, the point that Micky made about….

Deven McGraw - Center for Democracy & Technology – Director
That in some states consent would be required if it's in both?

Joy Pritts – ONC – Chief Privacy Officer
Yes. That should be forwarded immediately to Arien for their consideration.

Deven McGraw - Center for Democracy & Technology – Director
I would agree with that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'll see him at 3:00 West Coast time. I can tell him then.

Deven McGraw - Center for Democracy & Technology – Director
Thanks, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

Deven McGraw - Center for Democracy & Technology – Director
Do we want to open it up to public comment now?

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you see if anybody from the public wishes to make a comment?

Operator
We do have some questions.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. If that person or persons can please identify your name and your organization, and there's a three-minute limit, please.

Operator
Our first question comes from Saphel Korishi, who is a private investor … consultant.

Deven McGraw - Center for Democracy & Technology – Director
Go ahead.

Saphel Korishi – Private Investor
Yes. I guess, tomorrow, I'm really looking forward to kind of an expansion of some of these ideas. Regarding patient consent, is there a discussion of a registry of intermediaries and business associates like an accreditation database container that gets checked on every transaction? Thinking back to David's point that either the federal government or state HIEs handle this issue, but that kind of needs to be decided, I would think, sooner than later, to better define what's expected and the trust of that intermediary. I mean, it makes a big decision whether the federal government or the state level HIEs have to handle that type of accreditation.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, sir. Anybody else on the line?

Operator
Yes. Our next question comes from Archie Alexander, who is an independent consultant.

Archie Alexander – Independent Consultant
Yes. I have a couple questions, and I'll try to make them quick. With respect to intermediaries and consent, if you're going across interstate lines, I'm sure that you're going to either have a federal jurisdiction issue, as well as a state jurisdiction issue. Whose law will apply? Who is going to set the policies for this? And, finally, if you're in a state where a consent model is different from one state to another, will you have to get consent for that state as you go from one state to another state? And if you do, what happens if the individual says no? I don't want the intermediary to look at this. What happens to the routing and transmission?

Judy Sparrow – Office of the National Coordinator – Executive Director
Any comment on his comment?

Deven McGraw - Center for Democracy & Technology – Director

I think that these are issues that we're tackling, so I think it's just helpful to hear that feedback of things that we need to think about.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, Mr. Alexander. Anyone else?

Operator
Our next question comes from Ali Kalani, who is an independent consultant.

Ali Kalani – Independent Consultant
This is Ali Kalani. My question is about the … management information systems, which is a subset of … seven, how is it going to play … and what is going to be applicable across the nation.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you for that comment. Anyone else on the line?

Operator
Yes, our next question comes from Maurine Cooney from TRUSTe.

Maureen Cooney – TRUSTe – Chief Privacy Officer & VP Public Policy
Thank you very much. I appreciate that this meeting was open to the public today and really salute you for doing this and arranging your meetings in this way. Similar to other questions that have been asked, I appreciated the background on the NHIN Direct program, and the trust agreement that will be overseen by the coordinating committee. I think, if there's a place you can direct us to for more information on how that committee will operate, who the members are, and how monitoring will be done, that would be very helpful to better understand really accreditation of the companies that are participating and how their data management practices will be supervised.

I think, also, second to that question was really whether or not we would find in the DURSA the privacy and security features that the coordinating committing will be reviewing when they review the data management of those companies. Then, finally, I guess I had a question since all of this comes under what is a federal contract, if I understood the presentation. Is the information exchange now subject to the Privacy Act? Thank you very much, and thank you for all of your service on the taskforce. Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
You're welcome. Anybody else on the line?

Joy Pritts – ONC – Chief Privacy Officer
I'd like to answer to just the last question.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I was going to say, Joy, you should definitely answer that last one.

Joy Pritts – ONC – Chief Privacy Officer
I'm not going to answer all of them, but I will answer the last question because there were a lot of questions there, but the Privacy Act applies to the federal partners who have a data management system. The Privacy Act also applies to their contractors in certain circumstances when those contractors are acting on behalf. But as a general matter, just because a federal partner is part of an exchange does not mean that the other private parties are subject to the Privacy Act. They are subject to, depending on

what their status is and who they are, they may be subject to the HIPAA privacy rule. And they may be subject to state laws. Usually applied by the state in which they are practicing, if it's a provider.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. Thank you. Anyone else on the line?

Operator
Our next question comes from Christine Looney.

Christine Looney
Hello?

Deven McGraw - Center for Democracy & Technology – Director
Go right ahead.

Christine Looney
I am in compliance with the Regenstrief Institute, which, as you all probably know, has operated a health information exchange for more than ten years now, and we do have, I mean, we do see the PHI. And so one of the things, based on comments today, is I think it would be helpful to involve examples of entities in the workgroup, an entity who maybe just transmits data, an entity who is an intermediary that does see the PHI to say how does this work. Why does it happen that way? To help sort of the committee understand the processes and procedures existing and already in place.

The other piece is, I think, and there may be representatives on the committee that can help with this. But I also think there's an issue with what is technically feasible to create, develop, and track or what is the cost for the, you know, like one of the commenters mentioned some sort of massive database that was going to track consent. Well, what's the cost for that? Who is going to pay for that? So there are a lot of practical implications to policy decisions.

Deven McGraw - Center for Democracy & Technology – Director
Thank you.

Paul Egerman – eScription – CEO
Those are very interesting comments, Christine. I appreciate that. Maybe through Judy Sparrow, if you could send an e-mail to me, I'd like to see if we could get some of your input into our call tomorrow.

Judy Sparrow – Office of the National Coordinator – Executive Director
That's great. Actually, I think we've run out of time. If anybody does have comments, you can always e-mail them to me, and I'll make sure the committee gets to see them.

Paul Egerman – eScription – CEO
Yes, and we also have a chance for comments tomorrow. We're meeting tomorrow from 10:30 to—

Judy Sparrow – Office of the National Coordinator – Executive Director
To 2:00.

Paul Egerman – eScription – CEO
To 2:00, so we'll provide time for comments, but I would like to simply take this opportunity to first thank the members of the public who listen to our call and especially thank those of you who called in with comments and questions, all of which were extremely valuable, especially appreciate all the comments

and questions about authentication and make sure the participants should be the right people. Those are very valid comments. And also, of course, I want to thank the members of ONC: Joy Pritts, Judy Sparrow, Mariann Yeager, and there are probably several others whose names I should be mentioning. But I want to thank ONC and, of course, the members of the tiger team. Do you have anything you would like to add, Deven?

Deven McGraw - Center for Democracy & Technology – Director
No, that was very nice, Paul. Thank you, everybody. See you tomorrow.

Paul Egerman – eScription – CEO
Thank you very much. See you tomorrow.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Bye.

Public Comment Received During the Meeting

1. Hello, from a hospital perspective, I would appreciate guidance as to whether I purse the Exchange or Direct? I assume I do not use CONNECT? Help, thank you

2. I've been listening to this as setting policy around distributed, electronically, enforceable ID Management, Authentication, or Data Integrity, but have not heard about Authorization or Auditing (which, given HIPAA is key) - consideration of X.509 to also include SAML would seem key to distributed authorization and auditing.

3. Please see the method HL7 uses to assess a standards security considerations through risk assessment model. http://wiki.hl7.org/index.php?title=Cookbook_for_Security_Considerations

4. How can you make it convenient for the patient and still protect their information?

5. Medical Records Regulations cover integrity of medical records.

6. NHIN-Direct puts consent/authorization in the hands for the sender... don't send if you have not meet the requirements of LAW etc.

7. There is already HIPAA ++ and Breach Notification rules, with enforcement... what more is needed?

8. Isn't the "intermediary" being discussed an endpoint of a message? Thus, its two messages: 1. to the intermediary (opened or unopened) 2. to the "destination" - why not say messages "one hop" and declare them encrypted over the network fully? In addition, it would seem the existing requirement in HIPAA would require minimum exposure for use already. Scalability and flexibility need to be considered - addressing one "hop" at a time drives scalability and flexibility.

9. What is an intermediary? A Cisco router?

10. Certificate Granularity: Is there not a policy issue related to Certificate Granularity. For example if the policy is Patient can direct consent to the individual provider level...then the certificate granularity would have to be at the individual level not at the organizational level...

11. Isn't NHIN Direct an open, volunteer, collaborative effort (i.e. any entity can join) Thus, others can listen at it (to their own benefit) and insert their ideas (or keep them proprietary if they wish) - this type of effort is absolutely needed for a useful conversation (i.e. policy without reference implementation is a bad idea).